Buchanan

Michael McLaughlin, Esq.
Co-Chair, Cybersecurity and Data Privacy
michael.mclaughlin@bipc.com

1700 K Street, N.W., Suite 300
Washington, D.C. 20006-3807
T 202 452 5463

September 5, 2025

The Attorney General Mike Hilgers
Nebraska Attorney General's Office
1445 K St
Lincoln, NE 68508

Re: Notice of Data Security Incident

Dear Attorney General James:

I am writing to you on behalf of Sleepy Hollow Country Club ("Sleepy Hollow," "We," or "Our") in accordance with Neb. Rev. Stat. §§ 87-801 to 807. Sleepy Hollow experienced unauthorized access to its information technology (IT) systems. Based on our investigation, the personal information of one (1) Nebraska resident may be involved. This notice may be supplemented with any new significant facts learned subsequent to its submission.

In or around May 2025, Sleepy Hollow discovered suspicious activity that affected its IT systems. Upon discovering this activity, we immediately took protective actions to stop the unauthorized access, notified U.S. federal law enforcement, including the Federal Bureau of Investigation ("FBI"), assessed the security of our network and systems, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation to date indicates that some personal information may have been accessed by an unauthorized party. The personal information that could have been subject to unauthorized access included individuals' name and social security number.

On September 5, 2025, we began providing written notice of this incident to potentially affected individuals. The written notice is being provided in substantially the same form as the letter attached hereto as **Exhibit A**.

We have installed monitoring devices on our IT systems to detect suspicious activity. We are also working to implement additional safeguards and are providing potentially affected individuals one (1) year of complimentary credit protection and monitoring services through Privacy Solutions at no cost to the individuals.

If you have any questions or if I can provide additional information, please contact me.

Sincerely,

Michael G. McLaughlin
Outside Counsel for Sleepy Hollow Country Club

With a copy to: david.eapen@bipc.com; jillian.cash@bipc.com

EXHIBIT A

Sleepy Hollow Country Club

777 Albany Post Rd
Briarcliff Manor, NY 10510

September [__], 2025

Notice of Data Incident

Dear <<First Name>> <<Last Name>>:

Sleepy Hollow Country Club ("Sleepy Hollow," "we," or "us") is writing to inform you about a recent cybersecurity incident that may have impacted some of your personal information. The security of your personal information is very important to us, and we take the trust you place in us very seriously. We wanted to advise you about the incident and to offer you some resources you may find helpful.

What Happened? Sleepy Hollow detected unauthorized activity in our information technology (IT) systems. Upon discovering this activity, we immediately took protective actions to stop the unauthorized access, notified U.S. federal law enforcement, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation indicated that some of your personal information may have been accessed by an unauthorized party around May of 2025. At this time, we have no reason to believe your information has been misused; however, we are providing you notice out of an abundance of caution.

What Personal Information May Be Involved? The affected personal information may have included your [applicable data elements].

What We Are Doing. We are taking this incident very seriously. Upon detecting unauthorized activity in our IT systems, we took immediate protective actions to contain the activity and retained industry-leading cybersecurity specialists to investigate the incident, ensure the unauthorized access ceased, and use lessons learned to improve our systems' security posture. It is our priority to continue to evaluate and deploy the level of robust security protocols, continuous monitoring, and staff training needed to prevent and defend against sophisticated cybersecurity threats.

What You Can Do. Although we have no indication at this time of any misuse of your information, we have secured the services of Privacy Solutions to provide complimentary identity credit monitoring and identity restoration for 12 months at no charge to you. To enroll in the credit monitoring services at no charge, please visit www.privacysolutions.com and enter the following activation code, <<Activation Code>>, to activate your membership and start monitoring your personal information. Please note the deadline to enroll is <<Enrollment Deadline>>. Privacy Solutions provides credit monitoring through Equifax, credit report and score access, identity theft insurance with $0 deductible, Identity Restoration services, and dark web monitoring.

For More Information. We sincerely regret any inconvenience this incident may cause you. If you have questions regarding this incident or the services available to you, please call [phone number] (excluding major U.S. Holidays):
Eastern Time: Monday to Friday 9:00 AM to 5:00 PM.

Sincerely,

Sleepy Hollow Country Club

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Order Your Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Report Incidents. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft/. If you believe your identity has been stolen, the FTC recommends that you take these steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently (for streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/); and (2) file a local police report, obtain a copy of the police report, and submit it to your creditors and any others that may require proof of the identity theft crime.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert stays on your credit file for one year and is a free service that helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Consider Placing a Security Freeze on Your Credit File. You may place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require you to provide certain personal information and proper identification prior to honoring your request to place a security freeze on your account. For example, you may be asked to provide: (1) Your full name with middle initial and generation (such as Jr., Sr., II, III); (2) your Social Security number; (3) your date of birth; (4) addresses where you have lived over the past five years; (5) a legible copy of a government-issued identification card (such as a state driver's license or military ID card); and, (6) proof of your current residential address (e.g., current utility bill or account statement). Below is contact information for the three major credit bureaus:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

Additional Information.

Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Contact the District of Columbia Office of Attorney General for steps to avoid identity theft: (202) 727-3400, 400 6th Street, NW, Washington DC 20001, http://oag.dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Maryland Attorney General: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

Massachusetts Residents: You have the right to obtain a police report and request a security freeze (free of charge) as described above.

New York Residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-7889898; https://ag.ny.gov/. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.
North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401- 274-4400. 0 Rhode Island residents were notified of this incident.

South Carolina Residents: You can obtain information from the South Carolina Department of Consumer Affairs: 293 Greystone Blvd., Ste. 400, Columbia, SC 29210; 800-922-1594; www.consumer.sc.gov.

Texas Residents: You can obtain information from the Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621- 0508; www.texasattorneygeneral.gov/consumer-protection/.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

New Mexico: You have rights pursuant to the Fair Credit Reporting Act. These rights include knowing what is in your file and your credit score; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; to be told if information in your credit file has been used against you; as well as other rights. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. For more information about the FCRA, and your rights pursuant to the FCA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.